

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-003455

(43)Date of publication of application : 06.01.1999

(51)Int.Cl. G07D 9/00
G07D 9/00
G06F 17/60
G06F 19/00
G06K 17/00
G07F 7/08
G07G 1/12

(21)Application number : 09-156400

(71)Applicant : NEC CORP

(22)Date of filing : 13.06.1997

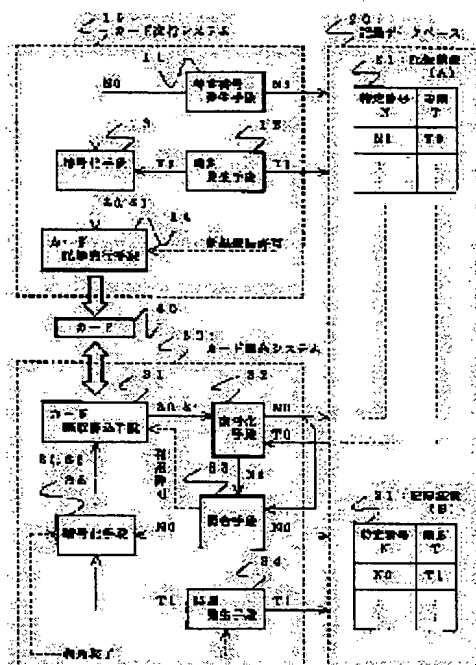
(72)Inventor : SATO YASUSHI

(54) ISSUING AND COLLATING METHOD FOR ELECTRONIC MONEY CARD AND ITS SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To make it difficult to forge or alter a card through recording medium.

SOLUTION: This method generates time data T0 that is a random number and a specific number N0 of a card 40 when a card is issued and records them on a recorder 21 outside the card 40, wherein the number N0 is a cipher data C1 with the data T0 as a key, and the data S1 and the number N0 are recorded on the card 40 and issued. At the time of using a card, the data T0 is retrieved from the recorder 21 based on the number N0 which is read from the card 40, the ciphered data is decoded by decoding the data S1 which is separately read from the card 40 with the data T0 as a key and the card is allowed to be used through collation coincidence. When the card 40 is returned, a cipher data S2 which is enciphered by a time data T1 that newly occurs is generated and recorded on the card 40 and the recorder 21. When an enciphered data is a card utilization number, alteration becomes even more difficult.



LEGAL STATUS

[Date of request for examination] 13.06.1997

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 2943861

[Date of registration] 25.06.1999

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁(JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 1 1 - 3 4 5 5

(43) 公開日 平成11年(1999)1月6日

(51) Int. Cl. ⁶	識別記号	F I
G 0 7 D 9/00	4 6 1	G 0 7 D 9/00 4 6 1 B
	4 3 6	4 3 6 Z
G 0 6 F 17/60		G 0 6 K 17/00 L
19/00		G 0 7 G 1/12 3 2 1 P
G 0 6 K 17/00		G 0 6 F 15/21 3 4 0 A
審査請求 有	請求項の数 1 9	O L
(全 1 8 頁) 最終頁に続く		

(21) 出願番号 特願平9-156400

(22) 出願日 平成9年(1997)6月13日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 佐藤 靖士

東京都港区芝五丁目7番1号 日本電気株式会社内

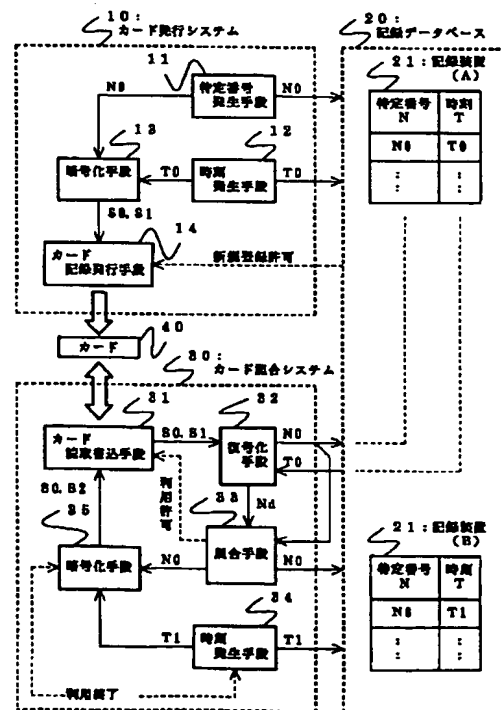
(74) 代理人 弁理士 後藤 洋介 (外2名)

(54) 【発明の名称】 電子貨幣カードの発行照合方法およびその方式

(57) 【要約】

【課題】 記録媒体によるカードの偽造または改ざんを困難にすること。

【解決手段】 カード発行の際には、乱数である時刻データ T0 とカード 40 の特定番号 N0 とを生成してカード 40 外の記録装置 21 に記録し、時刻データ T0 を鍵として特定番号 N0 を暗号化データ S1 とし、暗号化データ S1 と特定番号 N0 とをカード 40 に記録して発行する。カード利用の際には、カード 40 から読み取った特定番号 N0 に基づき記録装置 21 から時刻データ T0 を検索し、時刻データ T0 を鍵として別にカード 40 から読取った暗号化データ S1 を復号して暗号化されたデータを復号し、照合一致でカード利用を許可している。カード 40 の返却に際しては、改めて発生した時刻データ T1 により暗号化された暗号化データ S2 が生成され、カード 40 および記録装置 21 に記録される。暗号化されるデータがカード使用回数の場合、更に改ざんが困難である。



【特許請求の範囲】

【請求項 1】 記録媒体であるカードを発行し、このカードにより支払いの精算をする際、カードの照合を行う電子貨幣カードの発行照合方法において、カード発行システムと記録データベースとカード照合システムとを備え、前記カードは書込み読取り可能な記録媒体であり、前記記録データベースは各種データを記録する一方、検索を受けて送出し、前記カードを発行する際に、前記カード発行システムは、発行する前記カードを一意に特定する特定番号を発生すると共にランダムな数字の発行時乱数を発生し、次いで一方では前記発行時乱数を鍵データとして発生した前記特定番号および別に設定した特定数字の少くとも一方を暗号化した発行時暗号化データを作成し暗号化データにするこの前記発行時暗号化データと前記特定番号とを前記カードに記録して発行し、他方では発生した前記特定番号に対応して前記発行時乱数を乱数として前記記録データベースへ送って記録し、かつ前記カードを利用の際、前記カード照合システムは、カードから記録された特定番号および暗号化データを読み出し、この特定番号に基づいて前記記録データベースから前記特定番号に対応する乱数を索引し、前記カードから読み出された暗号化データをこの索引された乱数により復号し、得られた照合用復号符号を前記特定番号と照合して一致した場合に前記カードの利用を許可することを特徴とする電子貨幣カードの発行照合方法。

【請求項 2】 請求項 1 において、前記カード照合システムが、ランダムな数字の照合時乱数を発生し、前記カードの利用許可があった際に前記特定番号を前記照合時乱数により暗号化した照合時暗号化データを作成し、一方ではこの照合時暗号化データを前記カードに記録されている暗号化データに上書き記録し、他方では発生した前記照合時乱数を前記記録データベースへ送って記録されている乱数に上書き記録することを特徴とする電子貨幣カードの発行照合方法。

【請求項 3】 請求項 1 において、前記カードに記録する際、前記特定番号は特定の暗号化鍵により暗号化し、カード照合の際、この特定の暗号化鍵により復号して用いることを特徴とする電子貨幣カードの発行照合方法。

【請求項 4】 記録媒体であるカードを発行し、このカードにより支払いの精算をする際、カードの照合を行う電子貨幣カードの発行照合方法において、カード発行システムと記録データベースとカード照合システムとを備え、前記カードは書込み読取り可能な記録媒体であり、前記記録データベースは各種データを記録する一方、検索を受けて送出し、前記カードを発行する際には、前記カード発行システムは、発行する前記カードを一意に特定する特定番号を発生すると共にランダムな数字の発行時乱数を発生し、これら特定番号および発行時乱数を前記記録データベースへ送り、次いで記録データベースは、一方では受けた特定番号とこの特定番号に対応する

乱数として前記発行時乱数を記録格納すると共に、他方では受けた特定番号を発行時乱数を暗号化鍵として暗号化した発行時暗号化データを作成して前記カード発行システムへ送り、次いで、カード発行システムは、受けた前記発行時暗号化データを暗号化データとして前記特定番号と共に前記カードに記録して発行し、かつ前記カードを利用の際には、前記カード照合システムは、カードから記録された特定番号および暗号化データを読み出して前記記録データベースへ送り、次いでこの記録データベースは、この特定番号に基づいて前記記録データベースから前記特定番号に対する乱数を索引し、これら特定番号および乱数に基づいて特定番号を乱数により暗号化した照合用暗号化データを作成しこの照合用暗号化データをカードから読み出した前記暗号符号と照合して一致したことを前記カード照合システムへ送り、次いでカード照合システムが照合一致を受けた場合に前記カードの利用を許可することを特徴とする電子貨幣カードの発行照合方法。

【請求項 5】 請求項 4 において、前記カード照合システムが、ランダムな数字の照合時乱数を発生して前記記録データベースへ送り、前記カードの利用許可があった際に、前記記録データベースが、前記特定番号を前記照合時乱数により暗号化した照合時暗号化データを作成し、一方では記録されている乱数を照合時乱数に上書き記録し、他方では前記カード照合システムへ送り前記照合時暗号化データを前記カードに記録されている暗号化データに上書き記録することを特徴とする電子貨幣カードの発行照合方法。

【請求項 6】 請求項 1、2、3、4、または請求項 5 において、前記特定番号は、カードを発行する複数の前記発行装置それぞれで発生する通し番号と、前記カードを一意に特定できるように前記発行装置それぞれに予め付与された装置識別子とにより構成されていることを特徴とする電子貨幣カードの発行照合方法。

【請求項 7】 請求項 1、2、3、4、または請求項 5 において、前記乱数はその時点の時刻を参照した時刻データであることを特徴とする電子貨幣カードの発行照合方法。

【請求項 8】 請求項 1、2、3、4、または請求項 5 において、前記特定番号は請求項 6 に記載の通し番号および装置識別子により構成され、かつ前記乱数はその時点の時刻を参照した時刻データであることを特徴とする電子貨幣カードの発行照合方法。

【請求項 9】 請求項 1、2、3、4、5、6、7、または請求項 8 において、前記カード発行システムは、更に、利用実績の初期値を発生し、この利用実績の初期値データを前記カードに記録して発行すると共に前記記録データベースに記録し、かつ前記カード照合システムは、更に、利用毎に利用実績データを更新する一方、カード照合の都度、前記カードに記録されている利用実績

10

20

30

40

50

データを更新すると共に前記記録データベースの記録を更新することを特徴とする電子貨幣カードの発行照合方法。

【請求項 10】 請求項 9 において、前記特定番号に代り前記利用実績データが前記乱数により暗号化されることを特徴とする電子貨幣カードの発行照合方法。

【請求項 11】 記録媒体であるカードを発行し、このカードにより支払いの精算をする際、カードの照合を行う電子貨幣カードの発行照合方式において、カード発行システムと記録データベースとカード照合システムとを設け、前記カードは、書き込み読取り可能な記録媒体であり、前記カード発行システムは、発行する前記カードを一意に特定する特定番号をカードを発行する際に発生して出力する特定番号発生装置と、ランダムな数字の発行時乱数を発生して出力する発行時乱数発生装置と、カードを発行する際に発生した前記特定番号および前記発行時暗号化データを受け、前記発行時乱数を暗号化鍵として前記特定番号を暗号化した発行時暗号化データを作成しこの発行時暗号化データを出力する暗号化装置と、この暗号化装置から出力された発行時暗号化データを暗号化データとして前記特定番号と共に前記カードに記録して発行するカード記録発行装置と、カードを発行する際に発生した前記特定番号および前記発行時暗号化データを受けて前記記録データベースへ転送する第 1 のデータ通信装置とを備え、前記記録データベースは、前記特定番号と共に、乱数として前記発行時乱数を記録する記録装置と、指示を受けてこの記録装置のデータを検索し検索結果を出力するデータ検索装置と、このデータ検索装置を介して前記記録装置へ前記第 1 のデータ通信装置から受ける特定番号および発行時暗号化データを転送し、前記カード照合システムから受ける特定番号を前記データ検索装置に転送し検索された前記乱数を前記カード照合システムへ返送する第 2 のデータ通信装置とを備え、かつ、前記カード照合システムは、前記カードを利用の際にカードに記録された特定番号および暗号化データを読み出して送出する一方、カードの利用許可により所定のカード精算処理を終了した際にカードに所定データを記録するカード読取書込装置と、このカード読取書込装置から受けた特定番号を前記記録データベースへ送出し結果として受けた乱数を復号化鍵として前記特定番号を復号した復号符号を生成し出力する復号化装置と、この生成された復号符号を前記特定番号と照合して一致した際に利用許可を前記カード読取書込装置へ送る照合装置と、受けた特定番号を前記記録データベースへ転送しこの結果として受ける乱数を前記復号化装置へ送る第 3 のデータ通信装置とを備えることを特徴とする電子貨幣カードの発行照合方式。

【請求項 12】 請求項 11 において、前記カード照合システムがランダムな数字の照合時乱数を発生する照合時乱数発生装置を更に備え、前記暗号化装置は前記カー

ドの利用許可があった際に前記照合時乱数を暗号化鍵として前記特定番号を暗号化した照合時暗号化データを作成して出力し、前記カード読取書込装置はこの照合時暗号化データを前記カードに記録されている暗号化データに上書き記録し、第 3 のデータ通信装置は発生した前記照合時乱数を前記記録データベースへ送出し、前記記録データベースは記録されている乱数に受けた前記照合時乱数を上書き記録することを特徴とする電子貨幣カードの発行照合方式。

【請求項 13】 記録媒体であるカードを発行し、このカードにより支払いの精算をする際、カードの照合を行う電子貨幣カードの発行照合方式において、カード発行システムと記録データベースとカード照合システムとを設け、前記カードは、書き込み読取り可能な記録媒体であり、前記カード発行システムは、発行する前記カードを一意に特定する特定番号を前記カードを発行する際に発生し出力する特定番号発生装置と、ランダムな数字の発行時乱数を発生し出力する発行時乱数発生装置と、発行時乱数を暗号化鍵として前記特定番号を暗号化した発行時暗号化データを暗号化データとして前記特定番号と共に前記カードに記録して発行するカード記録発行装置と、前記特定番号および発行時乱数を前記記録データベースへ送りこの結果記録データベースから受ける前記発行時暗号化データを前記カード記録発行装置へ転送する第 1 のデータ通信装置とを備え、前記記録データベースは、受けた前記特定番号およびこの特定番号に対応する前記乱数を記録する記録装置と、前記カード発行システムおよび前記カード照合システムそれぞれとデータを授受する第 2 のデータ通信装置と、この第 2 のデータ通信装置を介して受ける前記特定番号に基づいて前記記録装置から対応する乱数を検索し出力するデータ検索装置と、一方では前記第 2 のデータ通信装置を介してカード発行システムから特定番号および発行時乱数を受け発行時乱数を暗号化鍵としてこの特定番号を暗号化した発行時暗号化データを作成して前記カード発行システムへ返送し、他方では前記第 2 のデータ通信装置を介して前記カード照合システムから受けた特定番号をこの特定番号に基づいて前記データ検索装置を介して検索により得た乱数を暗号化鍵として暗号化した照合用暗号化データを生成し出力する暗号化装置と、この暗号化装置から出力された照合用暗号化データと前記カード照合システムから受ける暗号化データとを照合し一致した場合に前記カードの利用許可を前記第 2 のデータ通信装置を介してカード照合システムへ送出する照合装置とを備え、かつ前記カード照合システムは、前記記録データベースとデータを授受する第 3 のデータ通信装置と、前記カードを利用の際に、カードに記録された特定番号および暗号化データを読み出し前記第 3 のデータ通信装置を介して前記記録データベースへ送り、この記録データベースの前記照合装置から照合一致を受け所定のカード精算処理を終

了した際にカードに所定のデータを記録するカード読取書込装置とを備えることを特徴とする電子貨幣カードの発行照合方式。

【請求項 1 4】 請求項 1 3 において、前記カード照合システムがランダムな数字の照合時乱数を発生し出力する照合時乱数発生装置を更に備え、この発生した照合時乱数を前記第 3 のデータ通信装置が前記記録データベースへ転送し、前記記録データベースでは、前記記録装置が前記第 2 のデータ通信装置を介して受けた照合時乱数により記録されている乱数を上書き記録更新し、暗号化装置が前記カードの利用許可があった際に、前記第 2 のデータ通信装置を介して受けた前記照合時乱数を暗号化鍵として前記特定番号を暗号化した照合時暗号化データを作成して出力し、この照合時暗号化データを前記第 2 のデータ通信装置が前記カード照合システムへ転送し、前記カード照合システムでは、前記カード読取書込装置が前記第 3 のデータ通信装置を介して受けた前記照合時暗号化データを前記カードに記録されている暗号化データに上書き記録することを特徴とする電子貨幣カードの発行照合方式。

【請求項 1 5】 請求項 1 1、1 2、1 3、または請求項 1 4 において、前記特定番号は、カードを発行する複数の前記発行装置それぞれで発生する通し番号と、前記カードを一意に特定できるように前記発行装置それぞれに予め付与された装置識別子とにより構成されていることを特徴とする電子貨幣カードの発行照合方式。

【請求項 1 6】 請求項 1 1、1 2、1 3、または請求項 1 4 において、前記乱数は、その時点の時刻を参照した時刻データであることを特徴とする電子貨幣カードの発行照合方式。

【請求項 1 7】 請求項 1 1、1 2、1 3、または請求項 1 4 において、前記特定番号は、請求項 1 5 に記載の通し番号および装置識別子により構成され、かつ前記乱数は、その時点の時刻を参照した時刻データであることを特徴とする電子貨幣カードの発行照合方式。

【請求項 1 8】 請求項 1 1、1 2、1 3、1 4、1 5、1 6、または請求項 1 7 において、前記カード発行システムは、更に、利用実績の初期値データを発生する利用実績初期値発生装置を備え、この利用実績の初期値データを前記カードに記録して発行すると共に前記記録データベースに記録し、かつ前記カード照合システムは、更に、利用毎に利用実績データを更新する利用実績更新装置を備え、カード照合の都度、カードに記録されている利用実績データを更新すると共に前記記録データベースの記録を更新することを特徴とする電子貨幣カードの発行照合方式。

【請求項 1 9】 請求項 1 8 において、前記特定番号の代りに、前記利用実績データが前記乱数を暗号化鍵として暗号化されることを特徴とする電子貨幣カードの発行照合方式。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】 本発明は、記録媒体であるカードを発行し、このカードにより支払いの精算をする際、カードの照合を行う電子貨幣カードの発行照合方式に関し、特に、カードに使用する記録媒体を単純化し、かつカードの偽造または不正使用を防止出来る電子貨幣カードの発行照合方式に関する。

【0 0 0 2】

10 【従来の技術】 従来、この種の電子貨幣カードの発行照合方式では、カードの認証に際して、カードの偽造または改ざんを防止するために、表面に顔写真を貼付けもしくは印刷した I D (個人識別) カード、I C (集積回路) による演算機能を内蔵するカードなどが用いられた。

【0 0 0 3】 表面の顔写真に対する技術が、例えば、特開平 8 - 3 0 5 8 1 6 号公報に記載されている。

20 【0 0 0 4】 この構成では、カード上の顔写真の特徴的な画像情報を、スクランブル圧縮による少い情報量でカードに記録することにより、照合装置で、顔写真の画像情報を高速で読み出し、カード上の顔写真が偽造・改ざんされていないかを迅速に判定している。

【0 0 0 5】 一方、I C 内蔵のカードについての技術が、例えば、特開平 8 - 2 8 7 2 0 2 号公報に記載されている。

30 【0 0 0 6】 この方式では、I C カードとサービス提供側のセンタとの両者に内蔵される暗号化関数が認証を偽造するものに盗まれてもカードの認証に対する安全性を高くするため、暗号化鍵と、センタから受けた乱数とを、暗号化関数に基づいてカード側が演算し、この演算結果をカードからセンタへ送り、カード側の演算結果とセンタで同様に演算した演算結果とをセンタで照合する場合に、センタ側からカードへ送る乱数のビット長をランダムに制御できるようにしたものである。

【0 0 0 7】

40 【発明が解決しようとする課題】 上述した従来の電子貨幣カードの発行照合方式のうち、上記公開公報に記載された顔写真の画像情報による方式では、カード上の画像情報とこの画像情報の圧縮データとが照合されるため、画像データの圧縮方式が盗まれた場合には、盗まれた圧縮方式を用いて改ざんされた顔写真の画像情報から得た圧縮データがカードに記録できるので、安全性に疑問があるという問題点がある。

【0 0 0 8】 すなわち、同一カード上のデータの整合性によってカードの認証を行う方式では、データの変換手段である暗号化手段が判明した場合にカードの偽造は比較的容易である。

50 【0 0 0 9】 また、上記公開公報に記載された I C カードによる方式では、カード内に複雑な機能をもたせるため、改ざんは困難になるが、カードそのもののコストが

かかり、例えば、プリペイドカードのように多量に使用してもらうには実用上の面で不向きであるという問題点がある。

【0010】本発明の課題は、上記問題点を解決して、カードに使用する記録媒体を単純化し、かつカードの偽造または不正使用を防止できる電子貨幣カードの発行照合方式を提供することである。

【0011】

【課題を解決するための手段】本発明による第1の電子貨幣カードの発行照合方法は、記録媒体であるカードを10 発行し、このカードにより支払いの精算をする際、カードの照合を行う電子貨幣カードの発行照合方法において、カード発行システムと記録データベースとカード照合システムとを備え、前記カードは書込み読取り可能な記録媒体であり、前記カードを発行する際に、前記カード発行システムは、発行する前記カードを一意に特定する特定番号を発生すると共に、ランダムな数字の発行時乱数を発生し、次いで一方では前記発行時乱数を鍵データとして発生した前記特定番号および別に設定した特定数字の少くとも一方を暗号化した発行時暗号化データを20 作成し、暗号化データにするこの前記発行時暗号化データと前記特定番号とを前記カードに記録して発行し、他方では発生した前記特定番号に対応して前記発行時乱数を乱数として前記記録データベースへ送って記録し、かつ前記カードを利用の際、前記カード照合システムは、カードから記録された特定番号および暗号化データを読み出し、この特定番号に基づいて前記記録データベースから前記特定番号に対応する乱数を索引し、前記カードから読み出された暗号化データをこの索引された乱数により復号し、得られた照合用復号符号を前記特定番号と30 照合して一致した場合に前記カードの利用を許可している。

【0012】この方法によれば、カードは、単に書込み読み出し可能な記録媒体でよい。また、各システムでの暗号化方式が固定していても暗号化鍵データが各カードにより異なるうえ、暗号化鍵データを記録保管する記録データベースをカード発行場所またはカード照合場所のいずれからでも離すことができるので、カード、カード発行システム、またはカード照合システムのみ在るデータだけでは認証可能なカードに改ざんすることは困難である。

【0013】また、上記第1の発明に対して前記カード照合システムが、ランダムな数字の照合時乱数を発生し、前記カードの利用許可があった際に前記照合時乱数を暗号化鍵として前記特定番号を暗号化した照合時暗号化データを作成し、一方ではこの照合時暗号化データを前記カードに記録されている暗号化データに上書き記録し、他方では発生した前記照合時乱数を前記記録データベースへ送って記録されている乱数に上書き記録している。

【0014】この構成により、記録データベースおよびカードの暗号化鍵データがカードを利用する度に更新され、共通の暗号化鍵データを使用していないので、暗号化鍵データが盗まれた場合でも暗号の解読を困難にしておき、改ざんによる安全性は更に高くなる。

【0015】本発明による第2の電子貨幣カードの発行照合方法は、カード発行システムと記録データベースとカード照合システムとを備え、前記カードは、書込み読取り可能な記録媒体であり、前記カードを発行する際には、前記カード発行システムは、発行する前記カードを一意に特定する特定番号を発生すると共にランダムな数字の発行時乱数を発生し、これら特定番号および発行時乱数を前記記録データベースへ送り、次いで記録データベースは、一方では受けた特定番号とこの特定番号に対応する乱数として前記発行時乱数を記録格納すると共に、他方では受けた特定番号を発行時乱数を暗号化鍵として暗号化した発行時暗号化データを作成して前記カード発行システムへ送り、次いで、カード発行システムは、受けた前記発行時暗号化データを暗号化データとして前記特定番号と共に前記カードに記録して発行し、かつ前記カードを利用の際には、前記カード照合システムは、カードから記録された特定番号および暗号化データを読み出して前記記録データベースへ送り、次いでこの記録データベースは、この特定番号に基づいて前記記録データベースから前記特定番号に対する乱数を索引し、これら特定番号および乱数に基づいて特定番号を乱数により暗号化した照合用暗号化データを作成しこの照合用暗号化データをカードから読み出した前記暗号符号と照合して一致したことを前記カード照合システムへ送り、次いでカード照合システムが照合一致を受けた場合に前記カードの利用を許可している。

【0016】この構成によれば、上記第1の発明から復号化手段を不要にしたにも拘らず、第1の発明同様な作用を有し、かつ暗号化手段が記録データベースに集中されているので、複数のカード照合システムを簡素化できる。

【0017】また、第2の発明においても、前記カード照合システムが、ランダムな数字の照合時乱数を発生して前記記録データベースへ送り、前記カードの利用許可があった際に、前記記録データベースが、前記照合時乱数を暗号化鍵として前記特定番号を暗号化した照合時暗号化データを作成し、一方では記録されている乱数を照合時乱数に上書き記録し、他方では前記カード照合システムへ送り前記照合時暗号化データを前記カードに記録されている暗号化データに上書き記録することにより、上記第1の発明同様の作用を有している。

【0018】また、乱数を時刻データとすることにより通常有する時計を利用することができるので、特別な乱数発生装置を不要にできる。また、カードの利用実績データを加味して整合性を調べることにより、カード内容

の改ざんなどによる不正使用を更に簡単に発見することができる。

【0019】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【0020】図1は本発明の実施の一形態を示す機能ブロック図である。図1に示された電子貨幣カードの発行照合方式では、カード媒体をカードとして新規にカードを発行するカード発行システム10、カードに関する各種データを記録格納する記録データベース20、およびカード利用の際、利用するカードを記録データベース20のデータに基づいて照合し、カード利用の可否を決定するカード照合システム30それぞれが設けられているものとし、カード40には一般の書き込み読取り可能な記録媒体が用いられるものとする。

【0021】カード発行システム10は特定番号発生手段11、時刻発生手段12、暗号化手段13、およびカード記録発行手段14を備えるものとする。記録データベース20は記録装置21を備えるものとする。また、カード照合システム30は、カード読取書込手段31、復号化手段32、照合手段33、時刻発生手段34、および暗号化手段35を備えるものとする。

【0022】カード発行システム10の特定番号発生手段11は、本カード発行照合システム内で多数のカードそれぞれに対して一意の番号を特定番号N0としてカード発行の際に発生するものとする。時刻発生手段12は、カード発行の時刻を認識できると共に、24時間にわたって異なる数字を順次発生するので乱数発生手段として用いられ、カード発行の際に発生している時刻データT0を暗号化手段13における暗号化鍵にするものとする。

【0023】また、暗号化手段13は、固定された特定暗号化鍵と、時刻発生手段12が発生した時刻データT0による暗号化鍵とにより、特定番号発生手段11が発生した特定番号N0を暗号化した暗号化データS0、S1それぞれを生成し、この暗号化データS0、S1をカード記録発行手段14へ送るものとする。

【0024】カード記録発行手段14は、記録データベース20から新規登録許可を受けた際、暗号化手段13から受ける暗号化データS0、S1をカード40の記録領域に記録した後、排出により発行するものとする。

【0025】記録データベース20の記録装置21は、特定番号Nとこの特定番号Nに対して適用される時刻データTとを記録する記憶領域を有し、まず、カード発行システム10で特定番号発生手段11が発生した特定番号N0と時刻発生手段12が発生した時刻データT0とを記録装置21(A)として記録するものとする。また、カード照合システム30でカード40の照合の際には、時刻発生手段34が発生した時刻データT1により記録装置21(B)に示されるように上書きされるもの

とする。

【0026】カード照合システム30のカード読取書込手段31は、利用するカード40をセットされた際に、カード40に記録されている暗号化データS0、S1それぞれを読み取り、復号化手段32へ送る。一方、カード読取書込手段31は照合手段33から利用許可を受けた際には暗号化手段35から受ける暗号化データS0、S2をカード40に上書き記録してカード40を排出することによりカード利用者に返却するものとする。

【0027】復号化手段32は、一方では特定暗号化鍵により暗号化データS0を復号して特定番号N0を生成し、生成された特定番号N0に基づいて記憶データベース20の記録装置21(A)から時刻データT0を検索して読取り受取る。復号化手段32は、他方では記録装置21から受ける時刻データT0を復号化鍵とし、カード読取書込手段31から受けた暗号化データS1を復号して復号符号Ndを生成し、照合手段33へ送る。復号符号Ndは、正常に認証できるカード40であれば特定番号N0である。

【0028】照合手段33は、一方では復号化手段32から復号符号Ndを受け、他方では復号化手段32で暗号化データS0から復号された特定番号N0を受けて両者を照合し、一致した特定番号N0を記録データベース20および暗号化手段35それぞれへ出力するものとする。また、照合一致は利用許可としてカード読取書込手段31へ通知されるものとする。

【0029】時刻発生手段34は、カード照合時刻を認識すると共に、乱数発生手段でもあり、24時間にわたり暗号化鍵となる数字を順次発生する。従って、時刻発生手段34は、カード照合の際に発生する時刻データT1を、暗号化鍵にすると共に記録装置21へ送るものとする。

【0030】暗号化手段35は、一方では照合手段33から照合一致した特定番号N0を受け、他方では時刻発生手段34が発生する時刻データT1を受け、カード発行システム10と同様、一方では固定された特定暗号化鍵により特定番号N0を暗号化した暗号化データS0、他方では時刻発生手段32が発生した時刻データT1を暗号化鍵として特定番号N0を暗号化した暗号化データS2、それぞれを生成し、カード記録発行手段14へ送るものとする。

【0031】時刻発生手段34から記録装置21へ送られた時刻データT1は記録装置21(A)における時刻データT0に上書きされることにより、記録装置21(B)に図示されるように時刻データTが更新される。

【0032】次に、図1に図2を併せ参照して、カード発行手順(A)およびカード照合手順(B)について説明する。

【0033】カード発行システム10において、カード発行要求が発生した際、まず特定番号発生手段11が特

定番号N0を発生し、かつ時刻発生手段12が時刻データT0を発生し(手順101)、発生した特定番号N0および時刻データT0を暗号化手段13および記録装置21それぞれへ送る。

【0034】暗号化手段13は、特定番号N0を、特定暗号化鍵により暗号化して暗号化データS0を作成する一方、時刻データT0を暗号化鍵として暗号化し暗号化データS1を作成し(手順102)、暗号化データS0、S1をカード記録発行手段14へ送る。一方、記録装置21では特定番号N0に対応する時刻データTの領域に時刻データT0を新規登録する(手順103)。

【0035】手順103で新規登録の際、特定番号N0で記録装置21に既に時刻データT-が登録済みのように新規登録不可能な場合(手順104のNO)、手順は手順101から再度、開始される。

【0036】手順104が“YES”で新規登録された場合、カード記録発行手段が、記録データベース20から新規登録許可を受け、暗号化手段13から受けた暗号化データS0、S1を新規カードに記録し排出することにより、カード40が発行され(手順105)、カード発行手順は終了する。

【0037】次に、カード照合システム30において、カード読取書込手段31にカード40を挿入して利用する際、カード読取書込手段31は挿入されたカード40から暗号化データS0、S1を読取り(手順111)、復号化手段32に送る。

【0038】復号化手段32では、受けた暗号化データS0から特定暗号化鍵により特定番号N0を再生し、この特定番号N0を記録データベース20へ送り、記録装置21の特定番号N0領域から時刻データT0を索引する(手順112)。

【0039】次いで、復号化手段32は、カード読取書込手段31から受けた暗号化データS1を記録装置21から索引した時刻データT0を暗号鍵にして復号することにより特定番号Ndを再生して(手順113)、照合手段33へ送る。

【0040】照合手段33は復号化手段32から受けた暗号化データS0から再生した特定番号N0と暗号化データS1から復号した特定番号Ndとを照合する

(手順114)。次いで照合手段33は、照合一致の場合(手順115のYES)、挿入されたカード40の利用許可をカード読取書込手段31へ送る(手順116)と共に、一致した特定番号N0を暗号化手段35へ送る。

【0041】この利用許可にしたがってカード40が利用され、例えば、精算により利用が終了した際、一方では、暗号化手段35が、時刻発生手段34で発生する新しい時刻データT1を受け、この時刻データT1を暗号化鍵にして既に照合手段33から受けている特定番号N0を暗号化し、新しい暗号化データS2を作成し(手順

117)、特定番号N0を特定暗号化鍵により暗号化した暗号化データS0と共にカード読取書込手段31へ送る。

【0042】また、カードの利用が終了した際、他方では、時刻発生手段34が発生する新しい時刻データT1と照合手段33が発生する特定番号N0とを記録データベース20が受け、記録装置21の特定番号N0領域で時刻データT1を上書きして更新登録する(手順118)。

【0043】また、暗号化データS0、S2を受けたカード読取書込手段31は、暗号化データS1に暗号化データS2を上書きして更新記録したカード40を排出することにより(手順119)、カード40をカード利用者に返却する。

【0044】上記手順115が“NO”で照合が不一致の場合、照合手段33は、カード読取書込手段31へ挿入されたカード40が不良として利用不許可を通知する(手順116)。

【0045】上記説明では、単に特定番号発生手段としたが、具体的には、システム全体でカードそれぞれに一意の番号を付与できるように、複数のカード発行システムがある場合、カード発行システムそれぞれに装置番号を識別できる識別子を設定して、この識別子と、これらカード発行システムそれぞれで発生する通し番号とを組合わせて特定番号とすることが、適切な手段として採用できる。また、上記時刻発生手段は、時刻を特定するために用いられる場合、変化する暗号化鍵として適切であるが、変化する暗号化鍵として用いるのみであれば、別の乱数発生装置により発生された乱数を利用してもよい。

【0046】上記説明では、特定番号を固定の暗号化鍵により暗号化データに変換してカードに記録したが、カード照合システムで復号化手段がない場合には暗号化できないこともあり、カードの特定番号は、そのまま、暗号化なしで記録することでもよい。

【0047】また、上記説明では毎度可変の時刻または乱数を暗号化鍵として特定番号を暗号化して、本発明の主目的である改ざんの困難さを得ているが、更に利用の都度変更のあるデータ、例えば利用実績を数値化した利用回数データを、特定番号の代わりに暗号化することにより、暗号化データをより複雑にすることができるので、改ざんをより困難にすることもできる。

【0048】すなわち、カードに付与される特定番号以外の各種データを、それぞれが異なる乱数を持つ暗号化鍵データによって暗号化され、この暗号化された暗号化データをカードに記録し、暗号化される各種データを記録データベースの特定番号領域それぞれに記録することにより、より一層、カードの偽造・改ざんを困難にする。

【0049】また、上記説明ではカードを挿入し排出す

るとしたが、カードの記録媒体上で書き込み・読取りするためにカードを固定する構造は自由であり、上記説明が本発明を限定するものではない。

【0050】

【実施例】

【第1の実施例】次に、上記図1の形態に基づく第1の実施例について図3および図4を参照して具体的に説明する。図示されるように、電子貨幣カードの発行照合システムは複数のカード発行システム110、一つの記録データベース120、および複数のカード照合システム130により構成され、遠隔地間でデータ通信網を介して相互接続しており、書き込み可能な記録媒体によるカード140が使用されているものとする。

【0051】まず、図3を参照して第1の実施例のカード発行システム110について説明する。

【0052】カード140を発行するカード発行システム110は、特定番号発生装置111、時刻発生装置112、利用実績初期値発生装置113、暗号化装置114、カード記録発行装置115、およびデータ通信装置116を備えているものとする。記録データベース120は、記録装置121、データ検索装置122、およびデータ通信装置123を備えているものとする。

【0053】特定番号発生装置111は、カード発行の際に発行されるカード140に対して通し番号N-を順次発生し、カード140にシステム内で一意のカード番号を付与するため、発行装置識別子M0を出力するものとする。通し番号N- および発行装置識別子M0 それぞれはカード発行の際に、暗号化装置114およびデータ通信装置116それぞれへ送られる。

【0054】時刻発生装置112は、現在時刻T0を時刻データT0として発生し、カード発行の際に暗号化装置114およびデータ通信装置116それぞれへ送るものとする。利用実績初期値発生装置113は、カード140が未使用で利用実績がないことを示す初期値データV0を発生して、カード発行の際に暗号化装置114およびデータ通信装置116それぞれへ送る。

【0055】暗号化装置114は、発生した通し番号N0 および発行装置識別子M0 による特定番号と時刻データT0 と、更に利用実績初期値データV0 とを受ける。

【0056】暗号化装置114は、システム固定の暗号化鍵を有し、特定番号発生装置111から受ける通し番号N0 および発行装置識別子M0 をこの固有暗号化鍵により暗号化して暗号化データS0 とする一方、時刻発生装置112から受ける現在の時刻データT0 を暗号化鍵とし利用実績初期値発生装置113から受ける利用実績初期値データV0 を暗号化して暗号化データS1 とし、これら暗号化された二つの暗号化データS0、S1 をカード記録発行装置115へ送るものとする。

【0057】カード記録発行装置115は、新規登録許可を記録データベース120から受けた際、セットされ

ているカード140の記録領域に暗号化装置114から受けた二つの暗号化データS0、S1を記録し、記録されたカード140を排出することにより発行する。

【0058】データ通信装置116は、カード発行システム110内と記録データベース120との間でデータ通信網を介してデータの授受を行う通信装置である。

【0059】記録データベース120は、上述されたように、カード発行システム110で発生した通し番号N0 および発行装置識別子M0 による特定番号と時刻データT0 と、更に利用実績初期値データV0 とを受ける。

【0060】記録装置121は、通し番号N、発行装置識別子M、時刻データT、および利用実績データとして利用回数データVを記録する記憶領域を、通し番号Nおよび発行装置識別子Mによる特定番号に対応して設けるものとし、カード発行の際にはカード発行システム110から受けたデータを記録する。

【0061】データ検索装置122は、一方ではカード発行システム110から発行登録のための記録要求を受けた際、該当領域にすでに記録済みの場合には新規登録不可をカード発行システム110へ通知する。他方、データ検索装置122は、図示されていないカード照合システム130から通し番号Nおよび発行装置識別子Mによる特定番号を受け、この特定番号に対応する領域を検索して結果をカード照合システム130へ送る。

【0062】データ通信装置123は、カード発行システム110内と記録データベース120との間でデータ通信網を介してデータの授受を行う通信装置であると共に、カード照合の際には、図示されていないカード照合システム130との間のデータ授受も行う。

【0063】次に、カード発行の際の動作手順について説明する。

【0064】カード発行システム110で発生した通し番号N0、発行装置識別子M0、時刻データT0、および利用実績初期値データV0は、データ通信装置116、123を介してデータ検索装置122へ送られ、データ検索装置122は記録装置121で通し番号N0 および発行装置識別子M0 に対応する領域に時刻データT0 および利用回数データV0 を登録して新規登録許可をカード発行システム110へ返送する。この際に、既に登録済みの場合にはカード発行システム110へ新規登録不許可が送られる。

【0065】カード発行システム110では、記録データベース120から新規登録許可があった際に、カード記録発行装置115が、カード140に暗号化データS3、S4を記録して排出することによりカード140を発行する。

【0066】次に、図4を参照して第1の実施例のカード照合システム130について説明する。

【0067】利用する際にカードを照合するカード照合システム130は、カード読取書込装置131、復号化

装置132、照合装置133、時刻発生装置134、利用実績更新装置135、暗号化装置136、およびデータ通信装置137を備えている。

【0068】カード読取書込装置131は、利用するカード140をセットされた際に、カード140に記録されている暗号化データS3、S4それぞれを読み取り、復号化装置132へ送り、利用許可を照合装置から受けた際には暗号化装置136から受ける暗号化データS3、S5をカード140に上書き記録し排出することにより、カード140をカード利用者に返却する。

【0069】復号化装置132は、一方では、特定暗号化鍵により暗号化データS3を復号して特定番号N0、M0を生成し、データ通信装置137へ送り、生成された特定番号N0、M0に基づいて記憶データベース120の記録装置121から時刻データT0および利用回数データV0を検索して読み取り受取る。

【0070】他方では、復号化装置132は、記録装置121から受ける時刻データT0を復号化鍵として、カード読取書込装置131から受けた暗号化データS4を復号して復号符号Vdを生成し、照合装置133へ送る。復号符号Vdは、正常に認証できるカード140であれば利用回数データV0である。

【0071】照合装置133は、一方で復号化手段32から受ける復号符号Vd、他方で記録データベース120から受ける利用回数データV0、両者を照合し、一致した際に利用許可をカード読取書込装置131へ送ると共に特定番号N0、M0を暗号化装置136とデータ通信装置137を介して記録データベース120とのそれぞれへ出力するものとする。

【0072】時刻発生装置134は、カード照合時刻を認識すると共に、乱数発生手段でもあり、24時間にわたり数字を順次発生する。時刻発生装置134は、カード照合の際に発生する時刻データT1を、暗号化鍵として暗号化装置135へ送ると共にデータ通信装置137を介して記録データベース120へ送り記録データを更新するものとする。

【0073】利用実績更新装置135は、カード利用の際して、照合された利用回数データV0を受け、1回を加算更新した利用回数データV1を発生し、暗号化装置135へ送ると共にデータ通信装置137を介して記録データベース120へ送り記録更新するものとする。

【0074】暗号化装置136は、一方で照合装置133から特定番号N0、M0を受け、他方で時刻発生装置134が発生する時刻データT1および利用実績更新装置135から更新された利用回数データV1を受け、カード発行システム10と同様に、一方では固定された特定暗号化鍵により特定番号N0、M0を暗号化した暗号化データS3、他方では時刻発生装置134が発生した時刻データT1を暗号化鍵として利用回数データV1を暗号化した暗号化データS5、それぞれを生成し、カー

ド読取書込装置131へ送るものとする。

【0075】データ通信装置137は、カード照合システム130内と記録データベース120との間でデータ通信網を介してデータの授受を行う通信装置である。

【0076】時刻発生装置134から送られる時刻データT1および利用実績更新装置135から送られる利用回数データV1は、データ通信装置137、123を介してデータ検索装置122へ送られ、記録装置121において、時刻データT0および利用回数データV0を上書きすることにより、時刻データT0および利用回数データV0それぞれの記録が時刻データT1および利用回数データV1それぞれに更新される。

【0077】次に、カード照合の際の動作手順について説明する。

【0078】カード読取書込装置131にカード140を挿入して利用する際には、カード読取書込装置131が挿入されたカード140から暗号化データS3、S4を読み取り、復号化装置132に送る。

【0079】復号化装置132では、受けた暗号化データS3から特定暗号化鍵により特定番号N0、M0を再生し、この特定番号N0、M0を記録データベース120へ送り、記録装置121の特定番号N0、M0対応領域から時刻データT0および利用回数データV0を索引する。

【0080】次いで、復号化装置132が、カード読取書込装置131から受けた暗号化データS4を記録装置121から索引した時刻データT0を暗号鍵として復号することにより利用回数データVdを再生し、利用回数データVdと共に、先に記録装置121から索引した特定番号N0、M0、時刻データT0、および利用回数データV0を、照合装置133へ送る。

【0081】照合装置133は、復号化装置132から受けるデータ、すなわち、暗号化データS3から再生した特定番号N0、M0により記録装置121から索引された利用回数データV0と暗号化データS4から復号した特定番号Ndとを照合する。次いで照合装置133は、照合一致の場合、挿入されたカード140の利用許可をカード読取書込装置131へ送ると共に、特定番号N0、M0を暗号化手段35へ送る。

【0082】この利用許可にしたがってカード140が利用され、例えば、精算により利用が終了した際、一方では、暗号化装置136が、更新された時刻データT1および利用回数データV1を受け、この時刻データT1を暗号化鍵として利用回数データV1を暗号化し、新しい暗号化データS5を作成し、特定番号N0、M0を特定暗号化鍵により暗号化した暗号化データS3と共にカード読取書込装置131へ送る。

【0083】また、カードの利用が終了した際、他方では、記録データベース120が、新しい時刻データT1と利用回数データV1とを受け、記録装置121の特定

10

20

30

40

50

番号N0, M0 領域で時刻データT1 および利用回数データV1 それぞれを上書きして更新登録する。

【0084】また、カード読取書込手段31は、暗号化データS3, S5 とを受けた暗号化データS4 に暗号化データS5 を上書きして更新記録したカード140を排出しカード利用者に返却することにより、カード140の利用を終了する。

【0085】〔第2の実施例〕次に、上記実施の形態とは異なる第2の実施例について図5および図6を参照して具体的に説明する。図示されるように、電子貨幣カードの発行照合システムは複数のカード発行システム210、一つの記録データベース220、および複数のカード照合システム230により構成され、データ通信網を介して遠隔地間で相互接続されており、書込み読取り可能な記録媒体によるカード240が使用されているものとする。

【0086】第2の実施例が第1の実施例と相違する点は、暗号化装置222を一つの記録データベース220に設け、複数のカード発行システム210およびカード照合システム230には復号化装置も備えないことである。

【0087】まず、図5を参照して第2の実施例のカード発行システム210について説明する。

【0088】カード240を発行するカード発行システム210は、特定番号発生装置211、時刻発生装置212、利用実績初期値発生装置213、カード記録発行装置214、およびデータ通信装置215を備えるものとする。記録データベース220は記録装置221、データ検索装置222、暗号化装置223、照合装置224、およびデータ通信装置225を備えるものとする。これら装置の基本機能は、上記第1の実施例と同一である。

【0089】特定番号発生装置211は、カード発行の際に発行されるカード240に対して通し番号N-を順次発生し、カード140にシステム内で一意のカード番号を付与するため、発行装置識別子M1を出力するものとする。通し番号N0 および発行装置識別子M1 それぞれはカード発行の際に、暗号化装置214およびデータ通信装置215それぞれへ送られる。

【0090】時刻発生装置212は、現在時刻T0を時刻データT0として発生し、カード発行の際にデータ通信装置215を介して記録データベース220へ送る。利用実績初期値発生装置213は、カード240が未使用で利用実績がないことを示す初期値データV0を発生して、カード発行の際にデータ通信装置215を介して記録データベース220へ送る。

【0091】データ通信装置215は、カード発行システム210内と記録データベース220との間でデータ通信網を介してデータの授受を行う通信装置である。

【0092】記録データベース220では、データ通信

装置225を介して、特定番号発生装置211から通し番号N0 および発行装置識別子M1、時刻発生装置212から時刻データT0、更に、利用実績初期値発生装置213から利用実績初期値データV0 それぞれを受け、暗号化装置223が、時刻データT0を暗号化鍵として利用実績初期値発生装置213から受ける利用実績初期値データV0を暗号化し、この暗号化された暗号化データS6を新規登録許可としてデータ通信装置225を介しカード発行システム210へ送る。

【0093】カード発行システム210では、カード記録発行装置214が、新規登録許可として暗号化データS6を記録データベース220から受けた際、この受けた暗号化データS6並びに特定番号発生装置211から受けた通し番号N0 および発行装置識別子M1、更に利用実績初期値発生装置213から受けた利用実績初期値データV0 それぞれを、セットされているカード240の記録領域に記録し、記録されたカード240を排出することにより発行する。

【0094】一方、記録データベース220では、暗号化装置222が、カード発行システム210から受けた通し番号N0、発行装置識別子M1、時刻データT0 および利用実績初期値データV0 それぞれをデータ検索装置222を介して記録装置221へ送り、記録装置221において通し番号N0 および発行装置識別子M1の特定番号に対して記録されるものとする。

【0095】次に、図6を参照して第2の実施例のカード参照システム230について説明する。

【0096】カード240の利用許可を認証するカード照合システム230は、カード読取書込装置231、データ通信装置232、時刻発生装置233、および利用実績更新装置234を備えている。また、記録データベース220は、図5と同様に記録装置221、データ検索装置222、暗号化装置223、照合装置224、およびデータ通信装置225を備えるものとする。これら装置の基本機能は、上記第1の実施例と同一名称の装置とほぼ同様である。

【0097】従って、動作手順にしたがって説明する。

【0098】カード読取書込装置231は、利用するカード240をセットされた際、カード240に記録されている通し番号N0 および発行装置識別子M1の特定番号、暗号化データS6、ならびに利用実績初期値データV0 それぞれを読取り、データ通信装置232を介して記録データベース220へ送る。データ通信装置232は、転送した通し番号N0 および発行装置識別子M1の特定番号をカード240への書込みのため保持するものとする。

【0099】記録データベース220では、データ通信装置225を介して暗号化装置223が通し番号N0 および発行装置識別子M1の特定番号、暗号化データS6、ならびに利用実績初期値V0 それぞれを、また照合

装置 2 2 4 が利用実績初期値データ V0 を、カード照合システム 2 3 0 から受取る。

【0 1 0 0】暗号化装置 2 2 3 は、通し番号 N0 および発行装置識別子 M1 の特定番号に基づいてデータ検索装置 2 2 2 を介して記録装置 2 2 1 を検索し、時刻データ T0 を得る。また、暗号化装置 2 2 3 は、上記カード発行の際と同様、時刻データ T0 を暗号化鍵としてカード照合システム 2 3 0 から受ける利用実績初期値データ V0 を暗号化し、この暗号化された暗号化データ Sd、正常であれば暗号化データ S6、を照合装置 2 2 4 へ送

る。

【0 1 0 1】照合装置 2 2 4 は、暗号化装置 2 2 3 から受ける暗号化データ Sd と、カード照合システム 2 3 0 から受ける暗号化データ S6 とを照合し、照合の一致により利用許可をデータ通信装置 2 2 5 を介してカード照合システム 2 3 0 へ送る。

【0 1 0 2】また、図示されていないが、この照合装置 2 2 4 が、通し番号 N0 および発行装置識別子 M1 の特定番号に基づいてデータ検索装置 2 2 2 を介して記録装置 2 2 1 を検索し得た利用実績初期値データ V0 と、カード照合システム 2 3 0 から受ける利用実績初期値データ V0 とを照合して調べる場合、先の暗号化データと二重に照合の一致を調べることになり、照合をより一層厳しくできる。

【0 1 0 3】カード照合システム 2 3 0 では、記録データベース 2 2 0 から受けた照合一致の信号により、時刻発生装置 2 3 3 は時刻データ T1、また、利用実績更新装置 2 3 4 は利用回数データ V1、それぞれをデータ通信装置 2 3 2 を介して記録データベース 2 2 0 へ送る。この際、データ通信装置 2 3 2 は、転送する利用回数データ V1 を保持するものとする。

【0 1 0 4】記録データベース 2 2 0 では、暗号化装置 2 2 3 が再び、時刻発生装置 2 3 3 から送られる時刻データ T1 および利用実績更新装置 2 3 4 から送られる利用回数データ V1 により、上記同様、時刻データ T1 を暗号化鍵としてカード照合システム 2 3 0 から受ける利用回数データ V1 を暗号化し、暗号化データ S7 を生成する。

【0 1 0 5】この暗号化された暗号化データ S7 が、データ通信装置 2 2 5、2 3 2 を介してカード照合システム 2 3 0 へ送られる一方、暗号化装置 2 2 3 により時刻データ T1 および利用回数データ V1 が記録装置 2 2 1 へ送られ、上書きすることにより、時刻データ T0 および利用回数データ V0 それぞれの記録が時刻データ T1 および利用回数データ V1 それぞれに更新される。

【0 1 0 6】他方、カード照合システム 2 3 0 では、データ通信装置 2 3 2 が暗号化データ S7 を受け、かつカード利用の終了を知られることにより、受けた暗号化データ S7 と保持している通し番号 N0 および発行装置識別子 M1 の特定番号、並びに利用回数データ V1 とを

カード読取書込装置 2 3 1 へ送る。

【0 1 0 7】カード読取書込装置 2 3 1 は、利用許可と利用終了とを受けた際、データ通信装置 2 3 2 から受ける暗号化データ S7、通し番号 N0 および発行装置識別子 M1 の特定番号、並びに利用回数データ V1 をカード 2 4 0 に上書き記録し排出することにより、カード 2 4 0 をカード利用者へ返却する。

【0 1 0 8】上記説明では、利用許可と利用終了との時期を分けて説明したが、システムの効率的な使用では、例えば精算による利用終了の際に、カードの照合によりカードの利用許可／不許可の認証が行われる。

【0 1 0 9】また、上述したように、暗号化する対象データは上記説明に限定されない。

【0 1 1 0】

【発明の効果】以上説明したように本発明によれば、次のような効果を得ることができる。

【0 1 1 1】第 1 の効果は、改ざんのためのカード上のデータ解析が困難なことである。

【0 1 1 2】その理由は、カード上に記録された暗号化データは、時刻データなどの乱数により、各カード、更に一つのカードでも利用の都度、異なる暗号化鍵が使用されているためである。

【0 1 1 3】第 2 の効果は、カード上のデータ解析ができて偽造が困難なことである。

【0 1 1 4】その理由は、記録データベースをカードの発行場所または照合場所と隔離し、更に、利用実績などの発行記録を暗号化データとするなどにより、偽造により暗号化データの整合性を得ることが困難なためである。

【0 1 1 5】第 3 の効果は、カードの製造コストが安くあがることである。

【0 1 1 6】その理由は、カードが単なる書込み読取り可能な安価な記録媒体でよく、カード認証のための特別な演算機能などのシステムを必要としないためである。

【図面の簡単な説明】

【図 1】本発明の実施の一形態を示す機能ブロック図である。

【図 2】本発明の実施の一形態を示すフローチャートである。

【図 3】本発明の第 1 の実施例のカード発行システムを示す機能ブロック図である。

【図 4】本発明の第 1 の実施例のカード照合システムを示す機能ブロック図である。

【図 5】本発明の第 2 の実施例のカード発行システムを示す機能ブロック図である。

【図 6】本発明の第 2 の実施例のカード照合システムを示す機能ブロック図である。

【符号の説明】

1 0、1 1 0、2 1 0 カード発行システム

1 1 特定番号発生手段

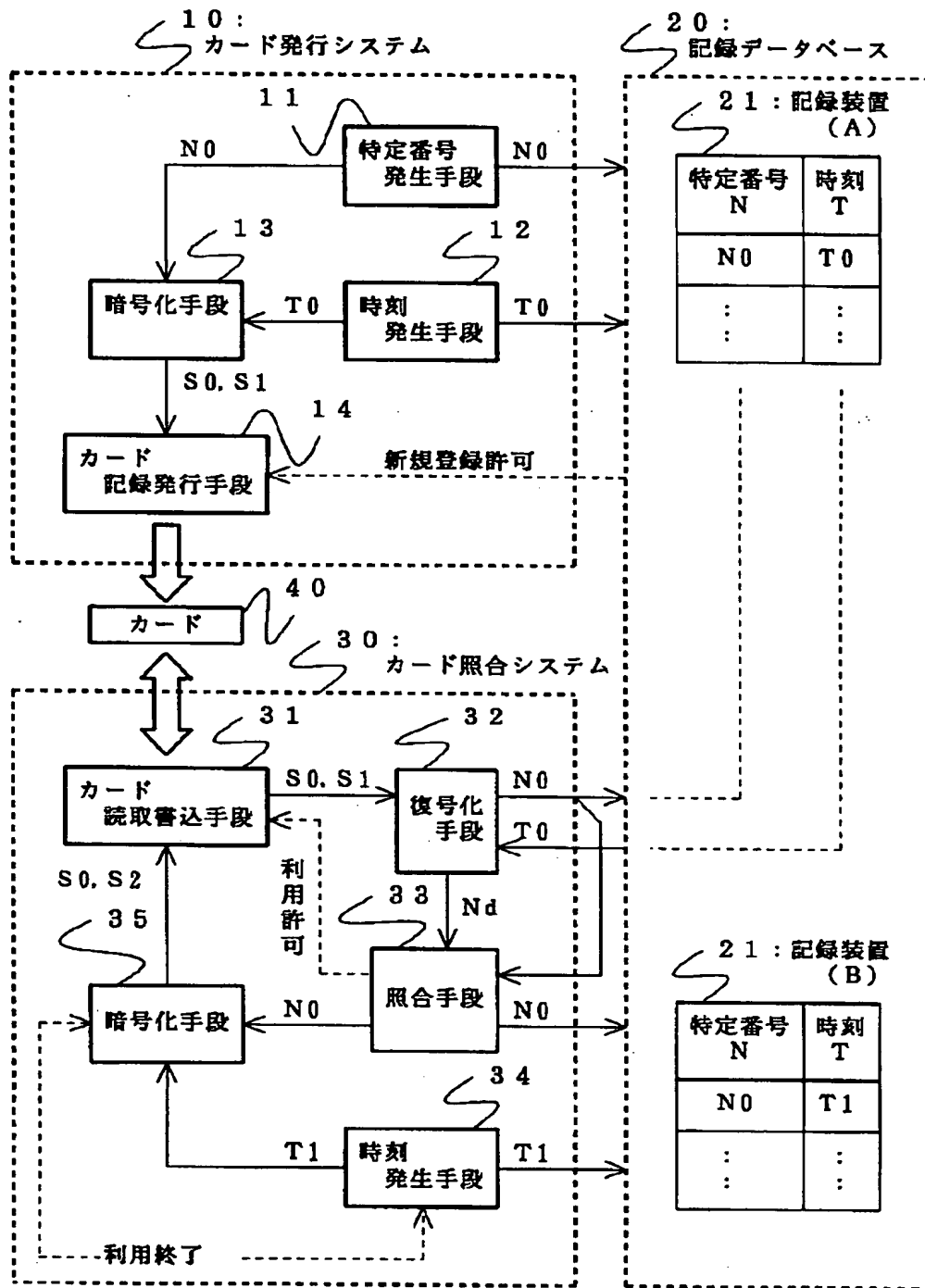
21

1 2 時刻発生手段
1 3、3 5 暗号化手段
1 4 カード記録発行手段
2 0、1 2 0、2 2 0 記録データベース
2 1、1 2 1、2 2 1 記録装置
3 0、1 3 0、2 3 0 カード照合システム
3 1 カード読取書込手段
3 2 復号化手段
3 3 照合手段
3 4 時刻発生手段
4 0、1 4 0、2 4 0 カード
1 1 1、2 1 1 特定番号発生装置

22

1 1 2、1 3 4、2 1 2、2 3 3 時刻発生装置
1 1 3、2 1 3 利用実績初期値発生装置
1 1 4、1 3 6、2 2 3 暗号化装置
1 1 5、2 1 4 カード記録発行装置
1 1 6、1 2 3、1 3 7、2 1 5、2 2 5、2 3 2
データ通信装置
1 2 2、2 2 2 データ検索装置
1 3 1、2 3 1 カード読取書込装置
1 3 2 復号化装置
10 1 3 3、2 2 4 照合装置
1 3 5、2 3 4 利用実績更新装置

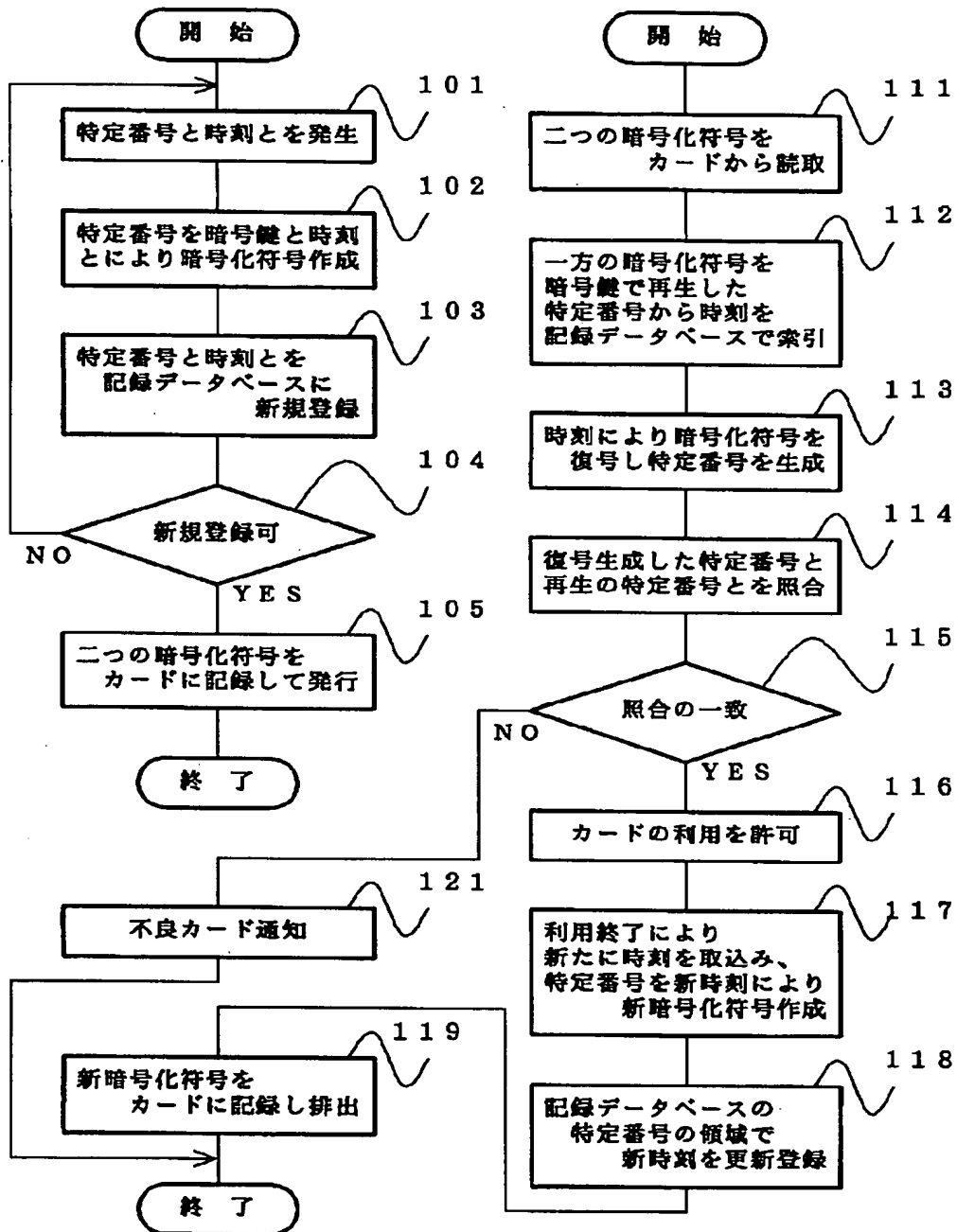
【図 1】



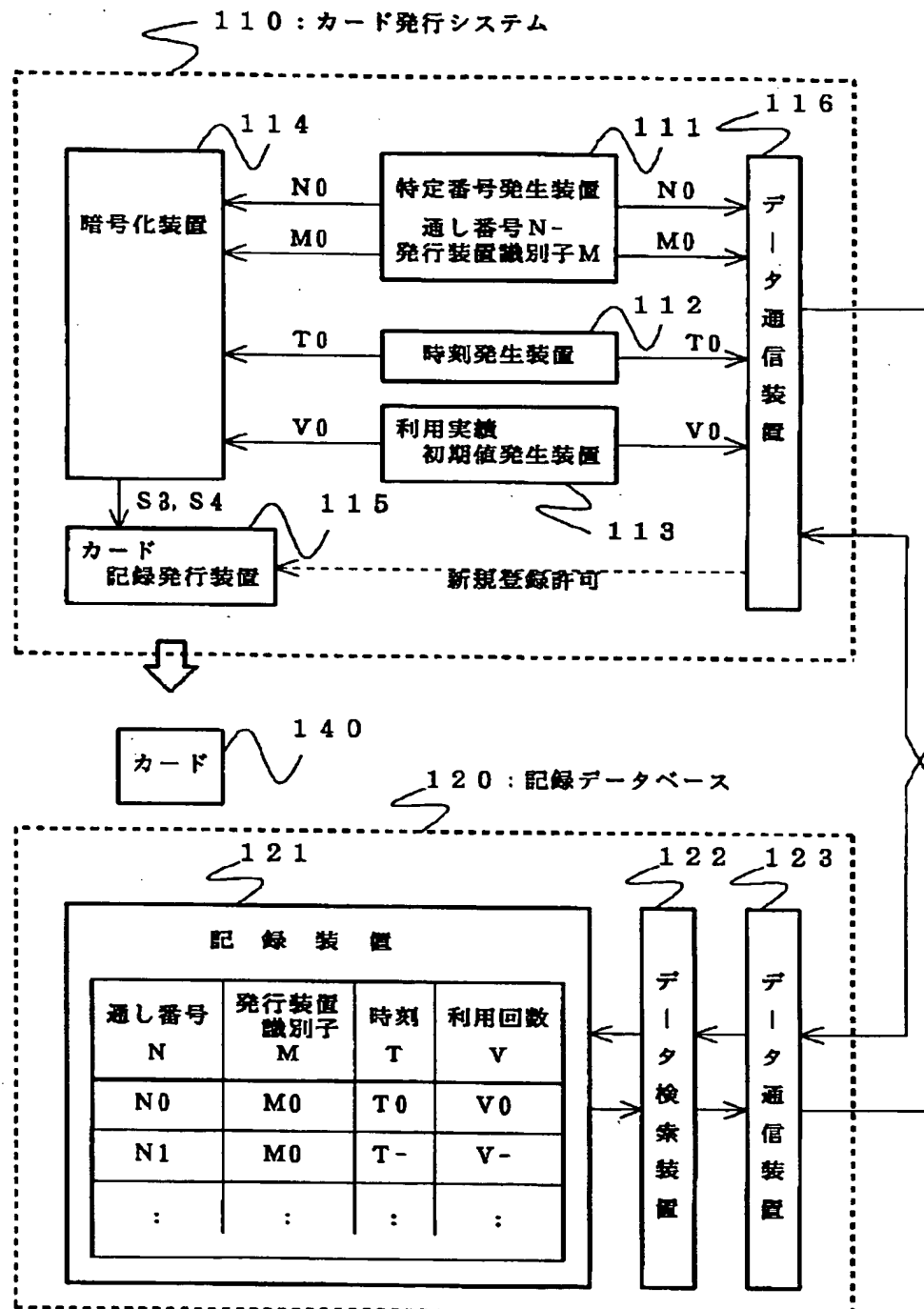
【図2】

(A) カード発行

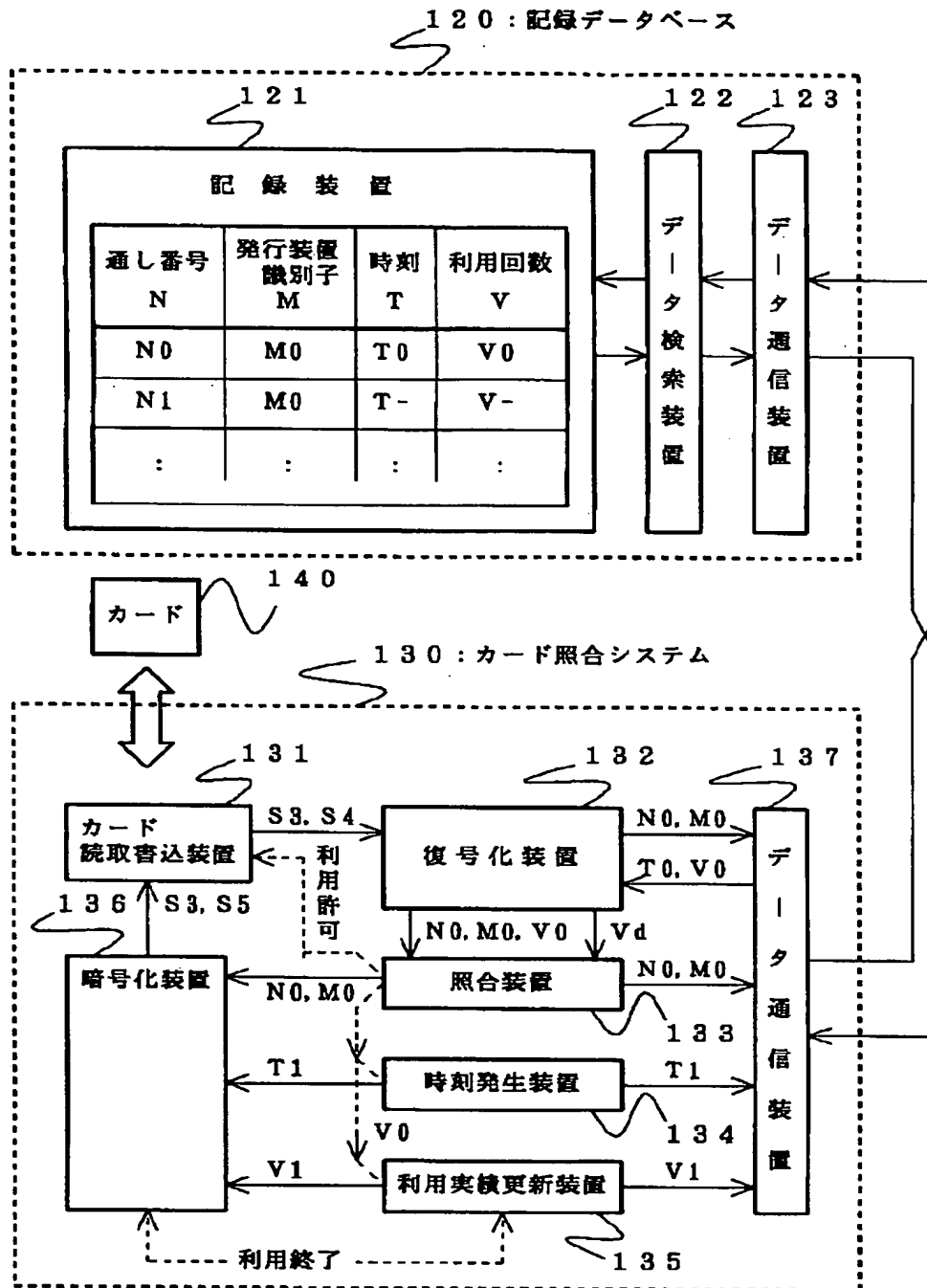
(B) カード照合



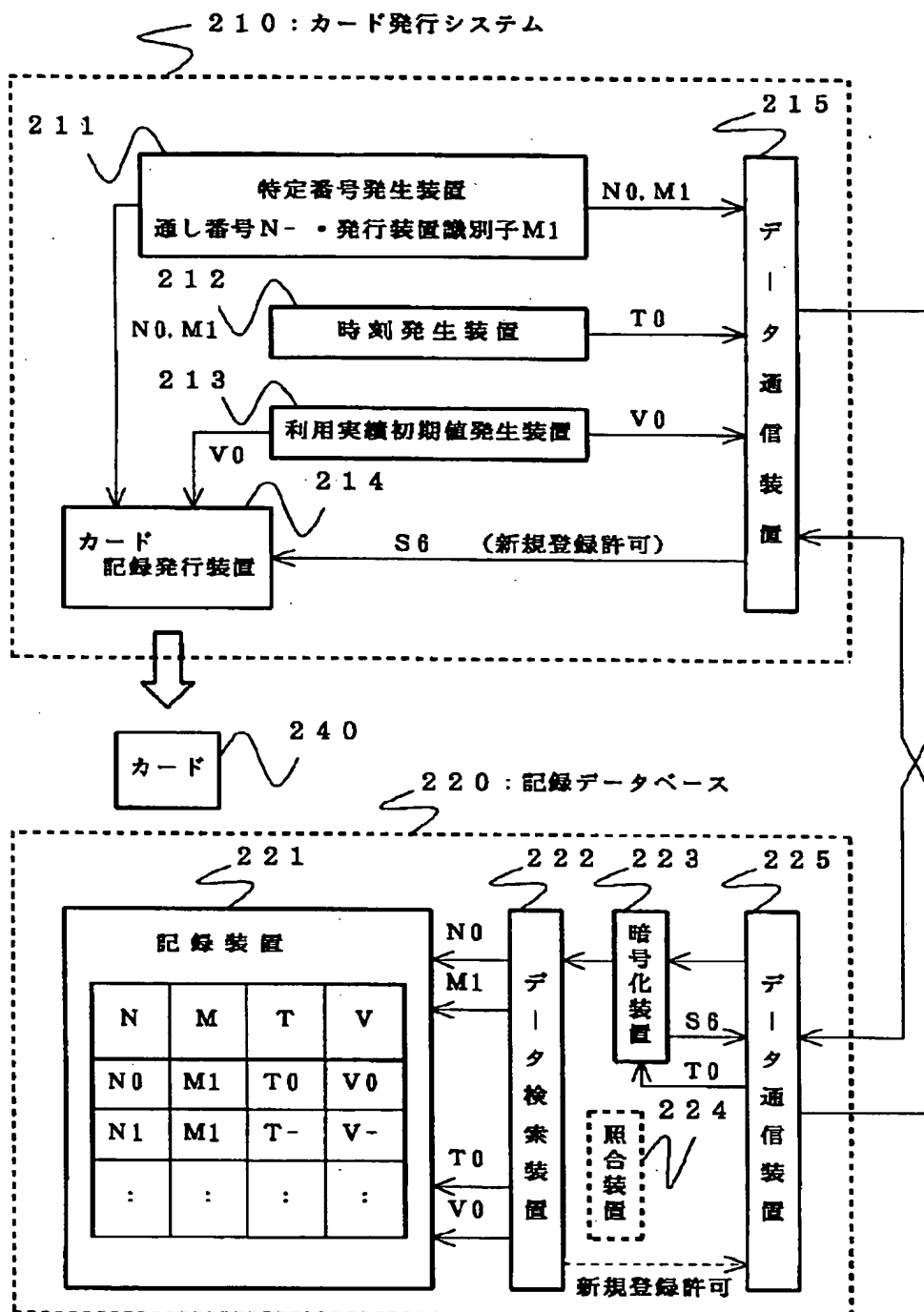
【図 3】



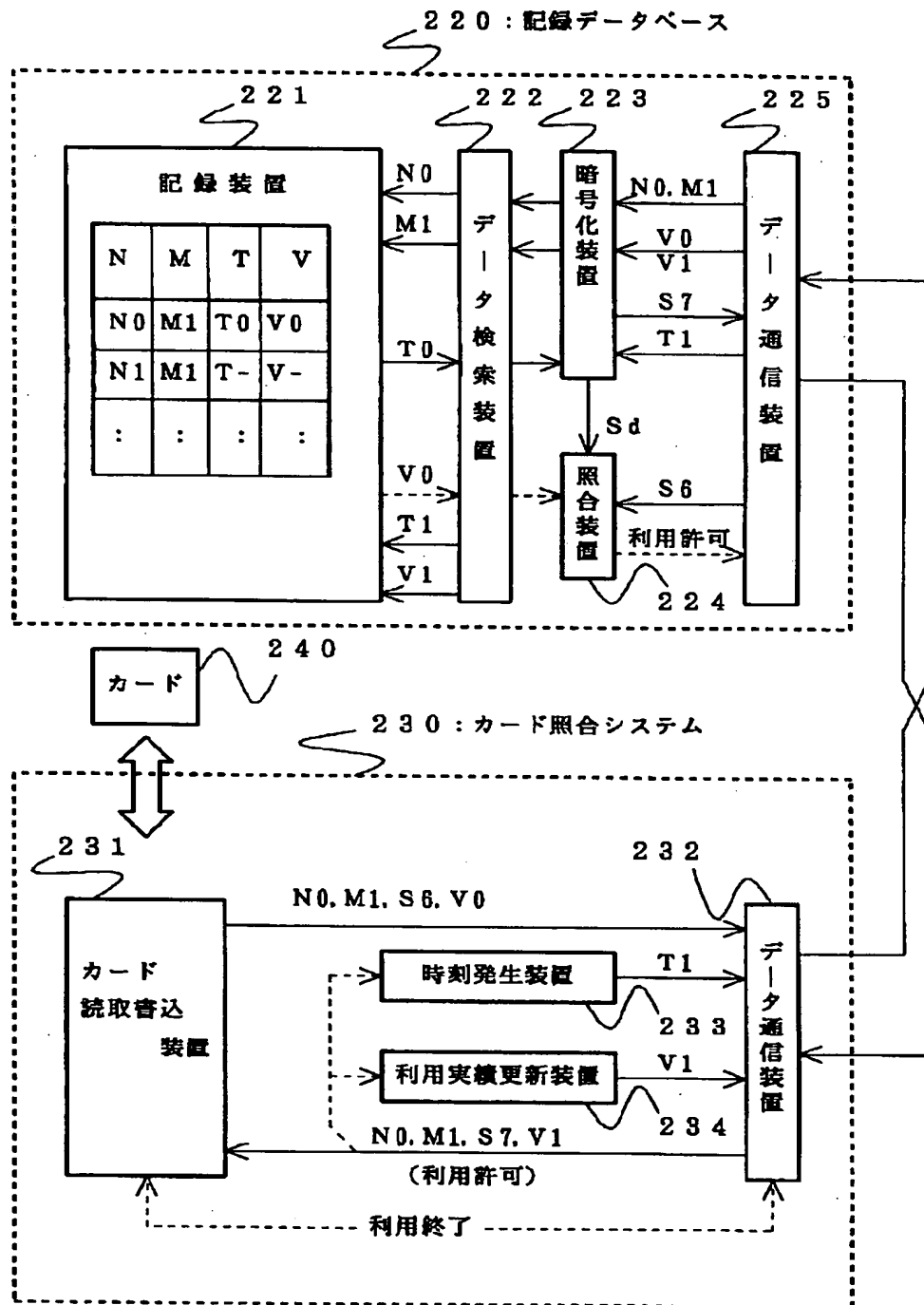
120: 記録データベース



【図5】



【図 6】



フロントページの続き

(51)Int.Cl.⁶

G 0 7 F 7/08

G 0 7 G 1/12

識別記号

3 2 1

F I

G 0 6 F 15/30

G 0 7 F 7/08

3 4 0

3 5 0 A

M